(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 263 248 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
04.12.2002 Bulletin 2002/49

(51) Int Cl.[7]: **H04Q 7/32**

(21) Numéro de dépôt: **02290959.2**

(22) Date de dépôt: **16.04.2002**

(84) Etats contractants désignés:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Etats d'extension désignés:
AL LT LV MK RO SI

(30) Priorité: **01.06.2001 FR 0107255**
21.02.2002 FR 0202207

(71) Demandeur: **Sagem SA**
75015 Paris (FR)

(72) Inventeur: **Chabanne, Hervé**
78200 Mantes la Jolie (FR)

(74) Mandataire: **Gorrée, Jean-Michel**
Cabinet Plasseraud,
84, rue d'Amsterdam
75440 Paris Cédex 09 (FR)

(54) Procédé d'activation d'une fonction dans un terminal abonné à un réseau

(57) Procédé pour activer une fonction logique dans un terminal abonné à un réseau, caractérisé en ce que l'opérateur du réseau émet, à destination du terminal, au moins un message spécial contenant les informations utiles à l'activation de la fonction logique dans le terminal, ledit message étant individualisé pour ledit terminal.

EP 1 263 248 A1

Description

[0001] La présente invention concerne des perfectionnements apportés au processus d'activation d'une fonction logique dans un terminal abonné à un réseau et notamment, bien que non limitativement, elle concerne des perfectionnements apportés, dans un réseau de communication sans fil, à l'activation d'une fonction logique dans un terminal mobile détenu par un abonné dudit réseau.

[0002] Actuellement, un terminal mobile peut être livré à l'abonné avec une ou plusieurs fonctions verrouillées (c'est-à-dire inutilisables) en relation par exemple avec des clauses contractuelles de l'abonnement liant l'abonné à l'opérateur du réseau ; mais ces fonctions initialement verrouillées peuvent devoir être déverrouillées ultérieurement (par exemple clause d'abonnement à action limitée dans le temps ; modification de l'abonnement ; etc...).

[0003] Toutefois, il convient que le déverrouillage de la fonction souhaitée ne puisse intervenir que pour un abonné déterminé et qu'avec l'accord de l'opérateur du réseau, et il convient d'empêcher des déverrouillages frauduleux.

[0004] C'est le cas en particulier pour le verrouillage dit "simlocking" liant un abonné à un opérateur de réseau donné.

[0005] Les opérateurs de réseaux de téléphonie mobile investissent dans l'équipement en terminaux en subventionnant une partie de leur coût. En contrepartie, au début de son utilisation, le terminal mobile est verrouillé ("simlocking") sur le réseau de l'opérateur spécifique, c'est-à-dire qu'il ne peut fonctionner que sur le réseau de l'opérateur qui l'a subventionné pour l'abonnement dans lequel il était inclus. Toutefois, ce verrouillage n'est prévu que pour une durée déterminée (par exemple 6 mois ou 1 an) et, à la fin de cette période, l'abonné peut demander à l'opérateur que son terminal mobile soit déverrouillé.

[0006] Aujourd'hui le verrouillage de sécurité ("simlocking") est mis en oeuvre dans le terminal mobile et, pour des raisons de coût, il s'agit en général d'un verrouillage essentiellement logique, c'est-à-dire faisant intervenir un logiciel ou agissant sur un logiciel, et de façon simplifiée, on peut considérer que le verrouillage du terminal mobile est obtenu par l'introduction, par l'opérateur du réseau, d'une information dérivée d'un code dans le terminal mobile lors de la mise en service de celui-ci.

[0007] Le moment venu, le déverrouillage est alors effectué par l'abonné lui-même qui introduit dans son terminal le code qui lui a été communiqué par l'opérateur du réseau lorsque l'abonné a fait part de son désir de déverrouillage. Le terminal mobile compare le code introduit par l'abonné avec l'information qu'il détient de façon secrète depuis sa mise en service et commande le déverrouillage donnant accès à d'autres réseaux.

[0008] Ce processus présente l'inconvénient de laisser à des fraudeurs la possibilité de remonter ("reverse engineering") jusqu'à l'information tenue en mémoire dans le terminal mobile et parfois d'en déduire le code devant être introduit pour provoquer le déverrouillage, ou parfois aussi de remplacer/modifier l'information mémorisée pour la faire correspondre avec un code choisi par le fraudeur. Le terminal mobile se trouve alors déverrouillé sans l'autorisation de l'opérateur du réseau.

[0009] Inversement, il peut être souhaité de verrouiller tout ou partie des fonctions d'un terminal mobile jusqu'alors actives, par exemple afin de neutraliser un terminal volé. Par analogie avec ce qui précède, cette neutralisation peut être faite en verrouillant ("simlocking") le terminal volé sur un réseau inexistant.

[0010] Plus généralement, dans le domaine informatique, il peut être souhaité d'activer une fonction logique dans un terminal informatique, par exemple pour autoriser ou interdire une connexion à un serveur ou sur un site Internet dans le cadre d'un abonnement.

[0011] L'invention a donc pour but de proposer un procédé d'activation d'une fonction logique perfectionné de manière à empêcher une activation frauduleuse de la fonction logique.

[0012] A cette fin, l'invention propose un procédé pour activer une fonction logique dans un terminal abonné à un réseau, lequel procédé se caractérise, conformément à l'invention, en ce que l'opérateur du réseau émet, à destination du terminal, au moins un message spécial contenant les informations utiles à l'activation de la fonction logique dans le terminal, ledit message spécial étant individualisé pour ledit terminal.

[0013] Ainsi, conformément à l'invention, toutes les informations nécessaires à l'activation de la fonction logique ne se trouvent plus présentes dans le terminal mobile dès la mise en service de celui-ci et il ne suffit plus de rentrer le code communiqué par l'opérateur du réseau pour commander l'activation de cette fonction : on accroît la sécurité en prévoyant l'introduction, dans le terminal, des informations - données et/ou programme - nécessaires à l'activation de la fonction uniquement au moment où celle-ci est souhaitée. Cette introduction s'effectue à distance par l'envoi d'un message spécial approprié au terminal.

[0014] Notamment, on peut prévoir que le susdit code soit communiqué au préalable à l'utilisateur du terminal par l'opérateur du réseau et que l'utilisateur l'introduise dans son terminal afin que ce dernier puisse lire le susdit message spécial lorsqu'il le reçoit de l'opérateur.

[0015] Mais, on peut aussi prévoir que le code ou une information équivalente soit contenu dans ledit message spécial : l'abonné n'a alors aucune autre démarche à effectuer que de demander à l'opérateur du réseau l'activation de la fonction logique dans son terminal ou bien, dans le cas d'un terminal devant être neutralisé (cas d'un terminal volé par exemple), le message spécial est émis par l'opérateur à sa propre initiative pour neutraliser ledit terminal.

[0016] Dans les deux cas, c'est la double introduction,

quasi simultanée ou simultanée, de deux types d'informations dans le terminal - d'un côté, le code qui est introduit par l'abonné qui le reçoit de l'opérateur du réseau ou bien qui est contenu dans le message spécial et, de l'autre côté, les informations contenues dans le message spécial envoyé par l'opérateur du réseau directement au terminal - qui valide l'activation de la fonction logique. Cette activation résulte ainsi de la volonté clairement exprimée de l'opérateur du réseau d'activer une fonction dans un terminal donné. Par exemple, dans le cas du verrouillage "simlocking" d'un terminal mobile, l'opérateur envoie dans le message spécial le nouvel état de verrouillage, cet état pouvant être par exemple "terminal déverrouillé" ou, par exemple encore, "terminal verrouillé sur un réseau inexistant" pour neutraliser un terminal volé.

[0017] D'une façon intéressante, les informations utiles à l'activation de la fonction logique peuvent comprendre des données et/ou, de façon encore plus sécuritaire, au moins un programme d'activation de ladite fonction. On est ainsi assuré que, quelles que soient les tentatives faites par un fraudeur avant que ces informations soient transmises au terminal par le message spécial, la fonction logique ne pourra pas être activée puisque les éléments logiciels nécessaires à cette activation ne sont pas présents dans le terminal.

[0018] Pour éviter qu'un message spécial destiné à un terminal donné soit intercepté par un fraudeur et réutilisé avec succès ultérieurement et/ou sur un autre terminal, on prévoit que le message spécial soit individualisé en outre en relation avec le terminal auquel il est spécifiquement destiné et sous au moins une donnée contenue dans le terminal et connue de l'opérateur du réseau.

[0019] De façon préférée dans ce cas, le message spécial est signé sous une clé privée de l'opérateur du réseau de manière à pouvoir être vérifié, une fois reçu par le terminal, sous une clé publique de l'opérateur du réseau qui est tenue en mémoire dans ledit terminal, l'activation de ladite fonction logique étant tributaire de la réussite de ladite vérification. On peut également envisager avantageusement que ladite fonction logique n'est activée que lorsque le terminal a vérifié que le message spécial était bien individualisé à son égard.

[0020] De façon également préférée, la donnée sous laquelle le message spécial est individualisé entre en compte dans le calcul de la signature. En particulier, lorsque le code est le seul élément d'individualisation et qu'il est communiqué par ailleurs à l'abonné, la signature porte à la fois sur le code et le message spécial.

[0021] Toutefois, il est souhaitable, pour améliorer la sécurité, que la donnée sous laquelle le message spécial est individualisé et/ou chiffré comprenne d'autres informations, et en particulier des informations caractéristiques du terminal et/ou tenues en mémoire dans celui-ci. Ainsi, le message spécial pourra en outre être individualisé par un des éléments suivants :

- un identifiant unique public et/ou
- un identifiant unique privé logiciel, c'est-à-dire connu seulement de l'opérateur du réseau (par exemple un numéro de série mis par le fabricant, qui n'est jamais communiqué à l'extérieur du terminal hormis vers l'opérateur), et/ou
- un identifiant unique privé matériel (par exemple peut être mis en oeuvre en plaçant dans le terminal un composant spécial prévu à cet effet).

[0022] Tous ces identifiants sont en pratique tenus en mémoire dans le terminal.

[0023] Dans un mode de mise en oeuvre préféré du procédé de l'invention, les messages spéciaux utiles à l'activation de la fonction logique sont envoyés chiffrés sous les identifiants précités et le code.

[0024] Enfin, toujours dans un mode de mise en oeuvre préféré du procédé de l'invention, l'activation de la fonction logique n'est réalisable que pendant un laps de temps prédéterminé, déclenché par exemple par la première occurrence de l'introduction du code dans le terminal par l'abonné et par la réception par le terminal du message spécial, le terminal étant de construction prévue à cet effet et calculant lui-même la fenêtre temporelle de validation de l'activation de la fonction logique.

[0025] Finalement, le processus d'activation de la fonction logique peut, conformément à l'invention, se dérouler comme suit en pratique. Les messages spéciaux utiles à l'activation de la fonction souhaitée sont envoyés, par l'opérateur du réseau à destination du terminal, chiffrés sous les susdits identifiants et le code. Après réception de ce message par le terminal, et éventuellement après l'introduction du code par l'abonné à l'aide du clavier du terminal, le terminal déchiffre le message spécial en mémoire volatile RAM et l'efface de sa mémoire non volatile (il en résulte que, si le terminal est recalé à zéro, l'effet du message spécial sera perdu). Le terminal disposant alors des données et/ou du programme nécessaire, l'exécution du programme d'activation de la fonction s'engage si le terminal a réussi la vérification de la signature grâce à la clé publique de l'opérateur qui est contenue dans sa mémoire.

[0026] Comme on l'a indiqué plus haut, une application tout particulièrement intéressante des dispositions de l'invention concerne le domaine de la téléphonie mobile et notamment le déverrouillage du terminal mobile préalablement verrouillé ("simlocking") comme exposé précédemment dans le préambule.

[0027] Dans ce contexte, pour, dans un réseau de communication sans fil, désactiver une fonction de verrouillage de type logique dans un terminal mobile détenu par un abonné dudit réseau, on peut procéder comme il suit :

- l'opérateur du réseau communique à l'abonné un code pour que celui-ci l'introduise dans son terminal mobile

et dans le même temps

- l'opérateur du réseau émet, à destination du terminal mobile, au moins un message spécial, tel qu'un message SMS, contenant les informations utiles à la désactivation de la fonction de verrouillage dudit terminal mobile, le message spécial, notamment SMS, étant individualisé.

[0028] Mais dans un autre mode opératoire, on peut prévoir que l'opérateur du réseau émet, uniquement à destination du terminal mobile, au moins un message spécial, tel qu'un message SMS, contenant les informations utiles à la désactivation de la fonction de verrouillage dudit terminal mobile, le message SMS étant individualisé pour ledit terminal mobile.

[0029] En effet, pour éviter qu'un message SMS destiné à un terminal mobile donné soit intercepté par un fraudeur et réutilisé avec succès ultérieurement et/ou sur un autre terminal, on prévoit que le message SMS soit individualisé en outre en relation avec le terminal mobile auquel il est spécifiquement destiné et sous au moins une donnée contenue dans le terminal.

[0030] De façon préférée, on peut faire en sorte que le message SMS inclut la signature sous une clé privée de l'opérateur du réseau téléphonique, tandis qu'une clé publique de l'opérateur est tenue en mémoire dans le terminal mobile de manière que le message SMS puisse être vérifié une fois reçu.

[0031] Grâce à un tel message signé, il devient aisé, pour l'opérateur, de rendre non fonctionnel un terminal mobile qui doit être éliminé du réseau (par exemple terminal volé).

[0032] Le message SMS pourra être individualisé avec :

- un identifiant unique public IMEI (International Mobile Equipment Identity ; norme ETSI GSM 02.16), et/ou
- un identifiant unique privé logiciel (c'est-à-dire connu seulement de l'opérateur du réseau) IDSOFT (par exemple un numéro de série mis par le fabricant, qui n'est jamais communiqué à l'extérieur du terminal mobile hormis vers l'opérateur), et/ou
- un identifiant unique privé matériel IDHARD (par exemple peut être mis en oeuvre en plaçant dans le terminal mobile un composant spécial tel que le composant DS 2401 Silicon Serial Number chip fabriqué par DALLAS Semi-Conductor).

[0033] Tous ces identifiants sont en pratique tenus en mémoire dans le terminal mobile.

[0034] Dans un mode de mise en oeuvre préféré du procédé de l'invention, les messages spéciaux SMS utiles à la désactivation de la fonction de verrouillage sont envoyés chiffrés sous IMEI, IDSOFT, IDHARD et CODE.

[0035] Enfin, toujours dans un mode de mise en oeuvre préféré du procédé de l'invention, la désactivation de la fonction de verrouillage n'est réalisable que pendant un laps de temps prédéterminé, déclenché par exemple par la première occurrence de l'introduction du code dans le terminal mobile par l'abonné et par la réception par le terminal mobile du message spécial SMS, le terminal mobile étant de construction prévue à cet effet et calculant lui-même la fenêtre temporelle de validation de la désactivation de la fonction de verrouillage .

[0036] Finalement, le processus de désactivation de la fonction de verrouillage peut, conformément à l'invention, se dérouler comme suit en pratique. Les messages spéciaux SMS utiles à la désactivation recherchée sont envoyés, par l'opérateur du réseau à destination du terminal mobile, chiffrés sous IMEI, IDSOFT, IDHARD et CODE. Après réception de ces messages SMS par le terminal mobile et après l'introduction du code CODE par l'abonné à l'aide du clavier du terminal mobile, celui-ci déchiffre les messages SMS en mémoire volatile RAM et les efface de sa mémoire non volatile (il en résulte que, si le terminal mobile est recalé à zéro, l'effet des messages SMS sera perdu). Le terminal disposant alors des données et/ou du programme nécessaire, l'exécution du programme de désactivation de la fonction de verrouillage s'engage si le terminal mobile a réussi la vérification de la signature grâce à la clé publique de l'opérateur contenue dans sa mémoire.

[0037] Comme cela a été précisé plus haut, les moyens de l'invention propres à commander une désactivation sécurisée du verrouillage d'une fonction du terminal mobile ont une application qui n'est pas limitée à la désactivation du "simlocking", mais peuvent trouver application en relation avec d'autres fonctions optionnelles prévues de construction, mais non initialement mises en service (par exemple fonction mains libres ; fonction de renvoi sur un autre terminal ; fonction d'affichage d'un numéro appelant ; ...).

[0038] Au surplus, les dispositions de l'invention ne se limitent pas à l'envoi, par l'opérateur vers le terminal mobile, de seuls messages SMS qui sont mis en oeuvre actuellement dans le réseau GSM ; elles pourront tout aussi bien être exploitées avec toutes sortes de messages pouvant être transmis dans le réseau WAP, ou encore d'autres réseaux futurs.

[0039] Enfin, on soulignera que, dans les explications qui précèdent, l'opérateur du réseau peut, dans certains cas, déléguer sa signature à une autorité compétente.

Revendications

1. Procédé pour activer une fonction logique dans un terminal abonné à un réseau, **caractérisé en ce que** l'opérateur du réseau émet, à destination du terminal, au moins un message spécial contenant les informations utiles à l'activation de la fonction logique dans le terminal, ledit message étant individualisé pour ledit terminal.

2. Procédé selon la revendication 1, **caractérisé en ce que** ladite fonction logique n'est activée que lorsque le terminal a vérifié que le message spécial était bien individualisé à son égard.

3. Procédé selon la revendication 1 ou 2, **caractérisé en ce que** le message spécial est signé sous une clé privée de l'opérateur du réseau de manière à pouvoir être vérifié, une fois reçu par le terminal, sous une clé publique de l'opérateur du réseau qui est tenue en mémoire dans ledit terminal, l'activation de ladite fonction logique étant tributaire de la réussite de ladite vérification.

4. Procédé selon l'une quelconque des revendications 1 à 3, **caractérisé en ce que** le message spécial est en outre individualisé par un des éléments suivants :

   - un identifiant unique public, et/ou
   - un identifiant unique privé logiciel connu uniquement de l'opérateur du réseau, et/ou
   - un identifiant unique privé matériel, tous tenus en mémoire dans le terminal.

5. Procédé selon l'une quelconque des revendications 1 à 4, **caractérisé en ce que** le message spécial comprend l'état d'un verrouillage dans le terminal.

6. Procédé selon la revendication 5, **caractérisé en ce que** l'état de verrouillage dans le terminal est propre à bloquer ledit terminal.

7. Procédé selon l'une quelconque des revendications 1 à 6, **caractérisé en ce qu'**en parallèle à la transmission du message spécial au terminal, un code est remis à l'utilisateur dudit terminal et **en ce que** l'utilisateur introduit ce code dans le terminal.

8. Procédé selon la revendication 7, **caractérisé en ce que** la signature sous une clé privée de l'opérateur du réseau est appliquée au susdit message spécial et au code.

9. Procédé selon l'une quelconque des revendications 1 à 8, **caractérisé en ce que** l'activation de la fonction logique est rendue possible par le terminal seulement pendant un laps de temps prédéterminé à compter de l'introduction du code par l'abonné ou de la réception du message spécial émis par l'opérateur du réseau.

10. Procédé selon l'une quelconque des revendications 1 à 9, **caractérisé en ce que**, après réception du message spécial émis par l'opérateur du réseau, le terminal déchiffre le message spécial en mémoire volatile RAM et l'efface de sa mémoire non volatile, ensuite de quoi le programme d'activation de la fonction logique s'exécute.

11. Procédé selon l'une quelconque des revendications 1 à 10, **caractérisé en ce que** le terminal est un terminal téléphonique mobile et l'opérateur du réseau est un opérateur de téléphonie mobile.

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 02 29 0959

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
X	WO 01 17297 A (QUALCOMM INC) 8 mars 2001 (2001-03-08) * page 5, ligne 25 - ligne 28 * * page 8, ligne 10 - ligne 18 * * page 8, ligne 26 - ligne 31 * * page 10, ligne 1 - page 11, ligne 8 *	1,2,4, 10,11	H04Q7/32
X	US 5 864 757 A (PARKER JOHN PATRICK) 26 janvier 1999 (1999-01-26) * colonne 4, ligne 5 - colonne 5, ligne 17 * * colonne 6, ligne 29 - ligne 67 *	1,2,4-8, 11	
X A	EP 0 796 023 A (NOKIA MOBILE PHONES LTD) 17 septembre 1997 (1997-09-17) * colonne 1, ligne 46 - ligne 57 * * colonne 4, ligne 35 - colonne 5, ligne 3 *	1-4,7,9, 11 5,6	
X	US 5 386 468 A (MOTOHASHI KAZUTOSHI ET AL) 31 janvier 1995 (1995-01-31) * colonne 7, ligne 29 - ligne 68 *	1-8,11	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7) H04Q G06F

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
BERLIN	20 juin 2002	Kampouris, A

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 02 29 0959

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

20-06-2002

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0117297	A	08-03-2001	US	6301484 B1	09-10-2001
			AU	7096200 A	26-03-2001
			EP	1208708 A1	29-05-2002
			WO	0117297 A1	08-03-2001
US 5864757	A	26-01-1999	AU	715488 B2	03-02-2000
			AU	1409997 A	03-07-1997
			CA	2239550 A1	19-06-1997
			EP	0867099 A2	30-09-1998
			JP	11501182 T	26-01-1999
			JP	3080409 B2	28-08-2000
			WO	9722221 A2	19-06-1997
			US	6124799 A	26-09-2000
EP 0796023	A	17-09-1997	FI	961154 A	14-09-1997
			EP	0796023 A2	17-09-1997
			US	6032038 A	29-02-2000
US 5386468	A	31-01-1995	JP	6097931 A	08-04-1994

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82